CENTURYTEL, INC.
OPERATING PROCEDURES & POLICIES

Overall Statement: CenturyTel, Inc. and its affiliates utilize reasonable and adequate safeguards and procedures to protect Customer Proprietary Network Information, including but not limited to: 1) employee training; 2) following "opt-out" notice rules; 3) electronic flagging of customer accounts; 4) password protection of account information; 5) seeking authorization and permission from customers prior to accessing customer information; and 6) adhering to internal compliance policies relating to customer privacy and information. Also, neither CenturyTel, Inc. nor its affiliates sell customer information to outside firms or vendors.

Specific Procedures: CenturyTel takes very seriously its obligation to safeguard CPNI from unauthorized access by employees and agents. As a result, we currently have the following specific procedures in place to ensure that we are in compliance with the rules in Subpart U of 47 C.F.R. Section 64:

(1) The company follows FCC rules relating to opt-out or opt-in notification provisions for its customers.
(2) The Company requires the use of security forms that must be filled out with employee/agent information and must be signed by that person and his supervisor prior to receiving any such login. CenturyTel agents must sign an Agency Agreement that deems our customer information as proprietary to CenturyTel, and states that they are bound by the same rules as our employees to keep such information confidential.
(3) Beginning with the employee job application, CenturyTel communicates to its employees the importance of protecting the confidentiality of all company-related information, including CPNI. During employee training and orientation, CenturyTel's Human Resources department trains each employee on privacy and security of customer information and the employee is provided a handbook that contains CenturyTel's policies on confidentiality of information.
(4) The company has conducted a comprehensive CPNI training session for senior management employees, which involved bringing CenturyTel's external FCC counsel to the company's headquarters to discuss the FCC's CPNI rules and appropriate compliance procedures.
(5) Privacy of customer information is reinforced among CenturyTel employees with special employee bulletins delivered via email, and documents contained on the company Intranet. In short, all employees having access to customer account information receive specialized training on when it is permissible to use, disclose or permit access to CPNI.
(6) The company has established provisions in its Corporate Compliance Program Procedures for dealing with potential unauthorized employee/agent breaches that could result in disciplinary action or criminal or civil liability. CenturyTel would also alert and work with the appropriate law enforcement agency to resolve the offense.

(7) To detect external (third party) breaches that may occur, CenturyTel utilizes Network Intrusion and Detection equipment which places network sensors at internet entry points into our internal networks. These sensors monitor incoming network traffic and generate real-time alerts 24 hours a day. Also, firewall devices are placed between un-trusted and trusted networks. These limit and restrict network traffic to only what is necessary for business purposes in a secure manner. Firewall logs are monitored daily for unusual and suspicious activity.

(8) CenturyTel's password management policy is included on the company's internal employee website for access by all employees and establishes the procedure for the creation, composition and maintenance of computer passwords. For online access to CPNI, each time a customer and/or an employee attempts to log-in, authentication is required. Currently, when those requirements are not met, then the attempt fails and access is denied. CenturyTel's procedures also limit the number of unsuccessful password/authentication attempts. After five unsuccessful attempts to enter a password, the involved account must be either suspended until reset by a system administrator, or temporarily disabled for no less than 15 minutes.

(9) A CPNI privacy flag, which contains the employee id and name, is attached to each account at the time the account is viewed. Additionally, CenturyTel validates employee access to systems which contain Subscriber Account Information on a quarterly basis. Employee access is granted based upon the employee's job functions and duties. If an employee changes jobs or departs from the company, his access is changed to a profile that fits his new job function or his access is revoked. Also, CenturyTel monitors calls and provides training on when customer approval is required before subscriber account information can be accessed.

(10) CenturyTel has developed a written Customer Service Practice on account confidentiality which sets forth company policy on using, disclosing or giving access to information regarding customers' accounts. Its objective is to identify the person inquiring or making a change to an account and to verify that person's authority to access the account in an effort to protect CenturyTel customer's rights to privacy.

(11) CenturyTel has a specific company policy related to critical or sensitive data developed by its Information Systems group. This policy is posted on the company's internal website accessible to all employees. It states, *inter alia*, that confidential information and other Company information that is not for public viewing must not be sent through email, must not be sent over the Internet, and must not be posted to any mailing list, newsgroup or other public area. This includes, but is not limited to, such items as CPNI and customer account passwords. The company's policy goes on to say that auto-forwarding of email to accounts outside the organization is not permitted. CenturyTel will take disciplinary action, up to and including termination, against any employee found to have violated these policies.

(12) CenturyTel has a policy related to critical or sensitive data, and this policy establishes uniform procedures for disposal of information, including proper erasure or destruction of removable electronic media (disks, tapes, CDs, DVDs,

etc.). Such policy is communicated to employees and available on the company's internal website for access by all employees.

(13) Any customer information saved or downloaded onto a laptop computer is password-protected and there are formal procedures in place to prevent password guessing attacks. For example, CenturyTel's password management policy is included on the company's internal employee website and establishes the procedure for the creation, composition and maintenance of computer passwords. CenturyTel's policy states that after five unsuccessful attempts to enter a password, the involved account must be either suspended until reset by a systems administrator, or temporarily disabled for no less than 15 minutes.

(14) To further reduce the likelihood of unauthorized online access, CenturyTel has enhanced its security measures for online access for our customers by requiring an additional verification to ensure the log-in of the customer matches the account being viewed. This additional verification measure requires the use of "cookies." This procedure utilizes the "cookie" stored on the end user's computer at the time the customer initiates the account or requests access to his or her account information. If cookies are blocked by the end-user, then access is denied.

(15) In the marketing service agreements it negotiates with its telemarketing vendors, CenturyTel requires its vendors to return all confidential information (including CPNI) to CenturyTel upon the request of CenturyTel or upon termination of the agreement. CenturyTel's legal department reviews compliance with this provision, and would follow up with a vendor if all or any part of any confidential information disclosed to the vendor were not returned as required.

(16) When fielding a request from a privileged caller (an attorney, law enforcement official, 911 operator, etc.), all such information requests are referred to the Legal Department. The Records Request Division within the Legal Department reviews each such request and requires proper legal documentation, such as a court order, before call detail information is released. The Records Request Division does not differentiate between requests by employees and "privileged" callers. All requests require proper legal documentation before call detail will be released. Further, the Records Request Division will only release call detail information to law enforcement officials, officers of the court or authorized government officials, and not directly to employees. If any record request appears to be out of the ordinary in any respect, the Records Request Division will ensure that one of the attorneys in the Legal Department conducts an additional review of the request before it is fulfilled.